MANAV RACHNA INTERNATIONAL UNIVERSITY

Short Synopsis
For

Ph. D. Program 2011-12

Optimized Secure Protocol for MANET through Biometric Approach

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
FACULTY OF ENGINEERING & TECHNOLOGY

Submitted by:

Name: Sherin Zafar
Registration No.:11/Ph.D/0015

Supervisor :
Name: Dr(Prof)M K Soni
Designation: Executive Director & Dean
FET(MRIU)

Joint-Supervisor
Name: Prof M.M.S Beg
Designation: Professor
FET(JMI)

ABSTRACT

This research work undertaken comprehends an impending accost of developing a secure protocol to sustain optimization and trust in MANET through crypt-biometric approach inculcating meta-heuristic algorithm. Meta-heuristics based genetic algorithm not only will help in maintaining Quality of Service(QOS) by selecting a fittest i.e. shortest route but also tends to overcome the security and privacy concerns that exist in biometric technology. Intelligent optimization approaches or meta heuristic algorithms like, genetic algorithm(GA), neural networks(NN) based on artificial intelligence(AI), particle swarm optimization(PSO) technique and simulated annealing(SA) in the recent years have well consigned QOS and privacy issues. Biometric authentication using fingerprint, facial, iris scan, voice recognition etc. have gain a lot of importance in recent years to provide security in MANET. Biometrics are more advantageous and secure as compared to prevailing data security techniques like password or token mechanisms. The foremost requirement of our protocol is to overcome various data attacks such as wormhole, cache poisoning, invisible node attack unauthorized data modification impersonation etc. that are caused by malicious node in MANET. This problem is tackled by crypt-biometric and trust application inculcated by meta-heuristic algorithm in our proposed approach which helps in securing ad-hoc networks.

Key words: Meta-Heuristic algorithm, user authentication, security challenges confronted by MANET, trust, biometrics, secure routing protocols in MANET, ICP.

CONTENTS

S. No.	Description	Page No.
1.	**Introduction** 1.1 Mobile/Motile Ad-hoc Networks(MANET) 1.2 Security Challenges Confronted By MANET 1.3 Current Secure protocols for routing in MANET	1-5
2.	**Literature Survey**	6-7
3.	**Description of Broad Area/Topic** 3.1 Quality Of Service(QOS) 3.2 Meta-Heuristic Algorithm 3.3 Genetic Algorithms(GA's) 3.3.1 Crossover Operations 3.4 Necessity of Biometrics Security	8-12
4.	**Problem Identification** 4.1 Procreation of Intelligent Optimization-Stationed Crypt-Biometric approach by employing Iris Connotation Process(ICP) 4.2 Objective of Study	13-14
5.	**Methodology to be Adopted** 5.1 Proposed Algorithm For Achieving QOS 5.2Process Describing Fundamental Population Engenderment And Chromosome Embodiment 5.3 Fitness/Competency Interpretation Of The Generated Population 5.4 Proposed algorithm for Crypt-Biometric Approach Inculcating Intelligent Optimization Technique	15-24

	5.5 Establishing Trust Forwarding Scheme **5.6 Ensuring Security of Data in MANET** **5.7 Security features accomplished by our proposed protocol** **5.8 Expected time frame required for developing optimized secure protocol for MANET through biometric approach**	
6.	**Proposed/expected outcome of the research**	**25**
7.	**References**	**26-28**

1.INTRODUCTION

1.1 Mobile/Motile Ad-hoc Networks(MANET)

An ad-hoc network is integrated robustly from scratch manipulating wireless connections and composed of mobile nodes. Mobile or motile ad-hoc networks will be used reciprocally in this short synopsis which signifies similar meaning i.e. operative or adaptable networks. MANETs other than standard data networks face various challenges due to their dynamic nature [9,23]. Content, pace of organization and less reliance on a permanent framework when grouped with conventional wireless networks are some of the unique features provided by MANET. Regardless, accessible distributed architecture, compelling network topology collated wireless mediocre ,confined battery, memory and computation power like unparallel characteristics lead to various consequential demands on security parameters of MANET. MANETs are required in those places where no permanent networking framework is available and time restrictions avoid developing such a framework, like military operations, law, enforcement, and various other rescue operations. Ad-hoc networks must be equipped with competence to emulate topology transitions since they have continuous dynamic connectivity between their various nodes .All accessible nodes in MANET as specified in fig.1 are conscious of every node inside their range of transmission.

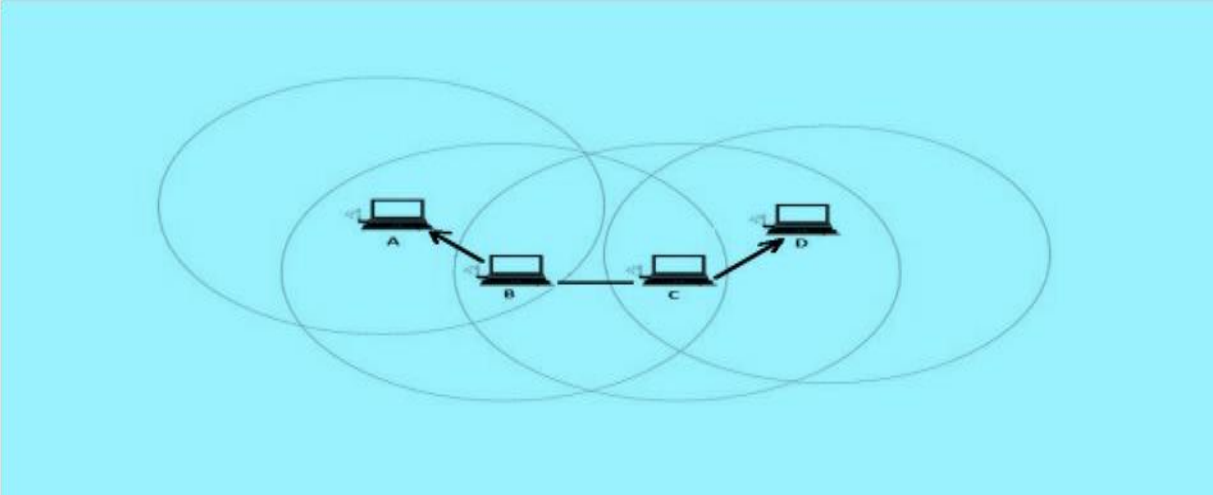


Fig 1.Example of Ad-hoc Network

1.2 Security Challenges Confronted By MANET

An ad-hoc network suffers from attacks from either direction, from any node, which is quite distinct as compared with fixed wired networks. That's why every node in MANET should be rigged to face an attack from any direction precisely or discursively. Any node in mobile/motile ad- hoc network(MANET) can be malignant therefore each node should be inclined not to trust on any node immediately. Central architecture deployed in the security elucidation can cause serious damages on the integral network if the centralized structure is afflicted so distributed networks are preferred so as to attain high availability(chief security concerning parameter for ad-hoc networks).

Below are discussed various active intrusions that ad-hoc network faces:

a. Black-hole Intrusion

This type of intrusion occurs when a malicious node suppose M on receiving a Route Request Packet(RREQP) revert backs a Route Reply Packet(RREPP) instantaneously, which formulates the information and can be transferred independently following the shortest route. So N receives Route Reply Packet(RREPP) reinstating M -> N. Then M accepts all the data coming from N.

b. Neighbour Intrusion

Neighbour and black- hole intrusion are common in a manner that they restrict the information packets from being forwarded to the destination(D) node. Unlike the black hole intrusion neighbour intrusion doesn't buckle nor abduct the information packets directed from the source (S) node. On dispatching false messages it abdicates the framework.

c. Worm-hole Intrusion

In wormhole type of intrusion two malignant nodes share an exclusive transmission association among themselves. Any one node apprehends the communication notifications of the ad-hoc network and forwards these notifications precisely to other malignant nodes. Worm-hole intrusion leads to various troubles in the network like snooping the network traffic, unscrupulously dropping the data packets and leading to man-in-the-middle intrusion against in motile ad-hoc network.

d. Denial-Of-Service(DOS) Intrusion

Denial of service intrusion occurs when malignant node spooks the network bandwidth [9]. The intruder embeds malicious packets inside the network so as to bestow valued network

assets like network bandwidth, memory or computation power. Routing table overflow and energy consumption attacks are some explicit occurrences of the Denial of service intrusion.

e. Message Betrayal Intrusion

The message betrayal intrusion targets the privacy of ad-hoc network. Confidential data like routing location of a network's node, its status ,private key information and watchword are disclosed through the malignant node directed towards various illegal nodes.

f. Hastening(Rushing) Intrusion

The hastening(rushing) intrusion targets on-demand ad-hoc routing protocols. They adopt exact annihilation on every node and when route to the destination(D) needs to be discovered, the source(S) node sends out the Route Request (RREQ) packet and every intermediary node proceeds the first un-equivalent information packet alone and dispose each equivalent information packet which appear next. These packets are delivered hurriedly by rushing intruders by jumping over some of the routing methods[27].

g. Jellyfish Intrusion

In jellyfish intrusion Route Request Packet(RREQP) and Route Reply Packet(RREPP) are transmitted regularly through the malignant node, but ahead of promoting it, it reprieve the information packets without particular apprehension for some period of time [27]. Its hard to comprehend this intrusion as the node attacks the forwarding association initially. The effect of jellyfish intrusion is minimal if the number of malignant nodes are less.

h. Byzantine Intrusion

Byzantine is one of impersonation intrusion as the malignant node behaves like another conventional node. Aberration updates are generated by transmitting incorrect routing information by the malicious node. Also, intruder accesses various confidential network resources in an unauthorized manner.

i. Blackmail Intrusion

Blackmail intrusion is relevant for routing protocols which exploit technique for the identification of nodes that can be malignant. These routing protocols broadcast information which tries to boycott the suspected node[17]. Blackmail intruder append various authorized nodes to the boycott list, and then they blackmail an authorized node.

1.3 Current Secure protocols for routing in MANET

The above discussed security demands lead to the advancement of various secure protocols for routing in MANET that aim to protect the network and hence enhance its performance. Defense mechanism of MANET against various types of attacks can be broadly categorized as: secure routing mechanism and security in packet transmission. Securing MANET can also divided into proactive approach which restricts an attacker from instigating attacks, by applying various cryptographic mechanism and reactive approach that explores and exposes various threats and their countermeasures[11] .We discuss the prevailing secure routing protocols in MANET and later will specify how their discrepancies can be avoided by this prospective approach.

► **Ariadne** : DSR prevents removing any current nodes or adding additional nodes along the network route by any intermediate node . A secure addendum to provide security in DSR is Ariadne [3].Prevention of wormhole intrusion and cache poisoning attack(attacker conveniently affect the libertine mode of updating a routing table , where a node updates its own cache on snooping a packet even if it is not on the path of that node) is not possible in Ariadne which leads to security breaches, also it suffers from complicated key exchange mechanism[3].

►**SAODV**: Protocol developed to provide security to AODV. SAODV substantiate non-erratic fields of route request packet (RREQP) and route reply packet (REPP) by employing digital signature which exploit one-way melange(hash) string(chains) to substantiate the hop tally (counts). Here, two malignant nodes affirm a link amidst them, and allow traffic through them. Public key cryptography compels eminent processing sustenance.

►***SAR :*** It employs a routing approach that amalgamate various security stages of nodes into prescribed routing metrics. SAR provides nothing regarding applying security stage as a metric and since no proper security approval is available route discovery system may abort, in spite of connectivity path between the relevant destination.

►***SEAD:*** A proactive secure protocol for routing in MANET stationed on DSDV-SQ-protocol. SEAD uses one-way melange(hash) chain for protection rather than traditional asymmetric encryption, which are engrossed quickly hence these chains should be either longer or librated regularly.

►***SDSDV:*** In SDSDV if no two nodes are in an association, a node propitiously recognizes a malignant routing amend (update) accompanying any sequence number or distance artifice, and exploits cryptographic technique for substantiation [25].SDSDV results in large network sustenance(overhead).

►***SLSP*** **:** It secures the identification and allotment of a link state information by appointing each node with a public/private key pair. SLSP is quite susceptible to intriguing attackers.

►***SRP*** **:**It establishes a security union(association) amidst the source(S) and the destination(D) node. SRP reveals network anatomy with un-encrypted routing path and affected by "invisible node attack"(any node that adequately cooperates without exposing its identity is an invisible node and the attack called as invisible node attack) [25] .

►***ARAN:*** It employs public key cryptography hence all nodes apperceive the actual next hop along a route from source(S) to destination(D). Consequence of above cryptography process is that ARAN faces number of issues regarding extra memory and large processing sustenance for encryption. Whether the perceived path is exemplary(optimal) is not guaranteed since ARAN doesn't avail hop count.[10].

2.LITERATURE SURVEY

Literature survey deals with succinctly demonstrating various explorations carried out for securing MANET including the numerous advances of biometric security, cryptography as well as exploring use of meta-heuristic algorithms. Many papers have been referred in this research work, with some discussed below:

Anand Patwardhan et al. [2] have led to the development of an advanced proposition protocol which leads to secure routing and established using AODV structure over IPv6.Intrusion Detection is reinforced by a response system for ad-hoc networks.

Zarza L et al. [29] have exemplified consideration of genetic algorithms as an assisting medium to conclude security protocols, hence leading to optimized elucidation for MANET. The paper optimizes problems by exploring security protocols refined for MANET as binary strings and applying genetic algorithm to genome assimilation .

Abhishek Roy and Sajal K Das.[1] have envisaged a protocol to attain QOS by generating near-optimal routes in MANET. The protocol conceives QOS designated instantaneous-best routes that pursue multicasting and avoid repetitions, even with rudimentary network knowledge which is specified by simulation results.

Rajaram.A and S.Palaniswami[21] have accomplished trust in MANET through a secure protocol which employs an approach cross-layer in nature aiming towards not only confidentiality but also results in greater authentication of packets in distinct layers.

Qinghan Xiao [20] has led to the development of a new approach for authentication by maintaining the biometric figures of all group participants. Distributed instead of a central authentication is employed. High security is provided through mutual cryptographic key applied for articulation inside a limited alliance and not suited for large enterprise management.

Jie Liu et al. [14] advised an optimum biometric-stationed constant substantiation(authentication) design for MANET which characterize through: user-to-device and device-to-network. The approach targets the user-to-device branch and optimally administer to accomplish authentication and employ biometrics to reduce the utilisation of network resources.

Ananda Krishna.B et al. [3] have characterized a model based on collective algorithms for encryption and decryption which is done done employing one of the algorithms selected in a random manner hence it's difficult to apprehend either algorithms or keys. For profound traffic network with great mobility ,the model performs better.

Shanthini.B et al. [24] have developed Cancellable Biometric-Based Security System (CBBSS) where biometrics cancellable in nature is employed for securing information in MANET. Fingerprint constituent of receiver are coupled with the tokenized melange data by applying an algorithm referred as inner-product . The result of this algorithm is stationed on a threshold value to develop a set of independent(private) binary cipher referred as cryptographic key in the system.

3.BROAD AREA OF RESEARCH

Featuring the various disadvantages that occur in the existing secure protocols of ad-hoc networks discussed in sec 1.3 of this research work leads in developing a secure protocol to sustain optimization and trust in MANET through crypt-biometric approach inculcating meta-heuristic based genetic algorithm which will embed the features of biometric technique, genetic algorithm and cryptography rendering a three level protection hence overcoming varied shortcomings of current secure protocols.

3.1 Quality Of Service(QOS)

As the ad-hoc networks are being utilised with various real-time applications , routing embedded with Quality of Service(QOS) must endeavour compelling challenges. Various multimedia services such as video conferencing(VC), real-time streaming(RTS) etc, demand stringent QOS assurance on various performance parameters like bandwidth and delay while transmitting data between various hosts. Various potent motile ad-hoc protocols have been developed keeping in mind the above mentioned real time applications , which will be able to arbitrate shortest best fittest routes that captivate various QOS parameters concurrently. Developing such protocols for optimizing various objectives, so as to enhance performance can be computationally fractious without the aid of meta-heuristic algorithms. Quality of service of MANET can recognized by quantitatively measuring in terms of various performance parameters like the throughput, average delay, average jitter, packet loss, end-to-end delay, packet delivery fraction and energy.

►**Throughput :** It's the measure of data rate i.e. bits per second consumed for transferring a packet from source to destination. Throughput is specified by the given formula:

Throughput(TP) = ∑ Size of Packet / (Arrival of Packet - Start of Packet)

where:

Size of Packet :packet size of the ith packet embracing the destination(D).

Start of Packet : time when the first(foremost) packet left the source(S).

Arrival of Packet: time when the last(aftermost) packet arrived.

►**Delay/latency :** It's the time taken by the packets to travel from the source to the destination. Latency can be further classified as: source- processing delay, propagation delay, network delay and destination processing delay. It is further specified by the given formula:

***Delay(D)*=** (Arrival of Packet - Start of Packet)/n

where:

Start of Packet : time when the first(foremost) packet left the source(S).

Arrival of Packet: time when the last(aftermost) packet arrived.

*n:*total number of packets.

►**Average Jitter :** It's the index of flexibility and stability of ad-hoc networks. It is specified by the given formula:

***Average Jitter*=** ((Arrival of Packet+1)- (Start of Packet+1))-((Arrival of Packet)-(Start of Packet))/n-1

►**Packet Loss :** Loss of packet occur due to various bit errors that occur during packet transmission. It is specified by the given formula:

***Packet Loss*=** (∑(Lost Packet Size/∑Packet Size)*100

►**Packet Delivery Fraction :** It is the ratio of the data packets forwarded to the destinations to those generated source .

►**End-to-End Delay :** It is the sum of processing delay, packet, transmission delay, queuing delay and propagation delay.

►**Energy :** It's the total amount of energy consumption for packets transmitted and packet receiving during the simulation.

3.2 Meta-Heuristic Algorithm

A **meta-heuristic** algorithm is an eminent method or heuristic accomplished to asset, initiate, or specify a lower-level strategy or heuristic (partial exploration algorithm) that administer an appropriately acceptable elucidation to an optimization dilemma, eminently with abridged or erroneous intelligence or confined data processing ability. Meta-heuristics are applicable for a range of complications that make insufficient hypothesis about the optimization dilemma being solved. The meta-heuristic algorithms can be categorized depending upon their various properties .The classification of these algorithms is specified below:

►G**enetic algorithms(GA)**

►Neural Network(NN) with Artificial Intelligence(AI)

►Simulated(Artificial) annealing(SA)

►Tabu-search or Tabu- exploration(TS or TE)

► Ant colony optimization(ACO)

►Evolutionary computation or Evolutionary estimation(EC or EE)

This research work will lead to the development of a protocol which will exploit intelligent optimization algorithm to enhance QOS parameters and privacy of biometrics for ad-hoc networks.

3.3 Genetic Algorithms(GA's)

Genetic algorithms [7] are algorithms under the category of estimating illustration determined through intrinsic transformation. These algorithms are accustomed by three imperative operators:

►**Selection** : This operator accomplishes its task by choosing the competent(fittest) distinctive chromosomes, designated as parents chromosomes that augment population of chromosome generation.

►**Cross-over** : This operator uses competent parent chromosomes of selection operator as its input and commix them to figure out child chromosomes for successive subsequent propagation.

►**Mutation** : Preserving genetic diversification of a population generation of individual chromosomes to next generation by altering from their original state their one/more gene values is done by mutation operator. Mutation takes place concurrently with evolution conceding a user -defined probability which should be kept as low as possible because keeping it high can lead to a primeval random exploration. This operator may cause genetic algorithm resulting in a preferred elucidation(solution) since here the elucidation may alter completely from the former. Mutation is applied basically if the algorithm gets stuck in condition referred as local minima, thus impeding chromosome population by adapting identical characteristics of each other resulting in reduced speed or even deterred evolution. Therefore it is referred in our algorithm which will be discussed later in the synopsis, that mutate if necessary.

3.3.1 Crossover Operations

Crossover methods, 2-bit and Modifying (Adaptive) crossovers are elucidated below:

►**2-bit Crossover:** Choose the parents required by the GA from the population generated, depending on their rank accomplished in the selection operation. Irregularly two bits are selected in parent chromosomes [5][28].

The nodes betwixt the selected bits are recurred to engender the descendants chromosome. The process of 2-bit crossover is depicted in fig.2.

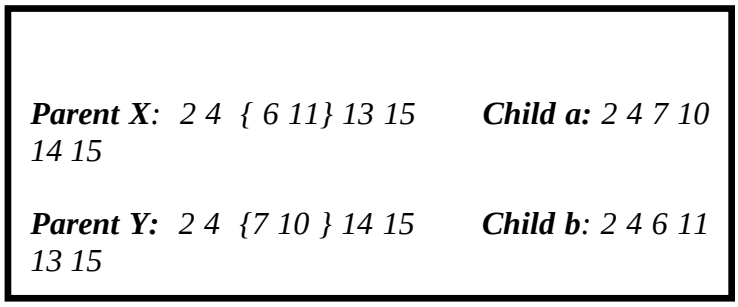


Fig.2 2-bit Crossover Operation

►**Modifying Crossover: A** customary nodes set € is established subsequently from preferred parents X and Y, by detecting all the compatible nodes exempting source node and destination node [5][28]. A congruous node is selected which is nearby the source(S) node, termed as a crossover point (for € >1, building block inference) from €.Then crossover operation is applied on the part after X and Y as specified by fig.3 where source node is 2 and destination node is 15 :

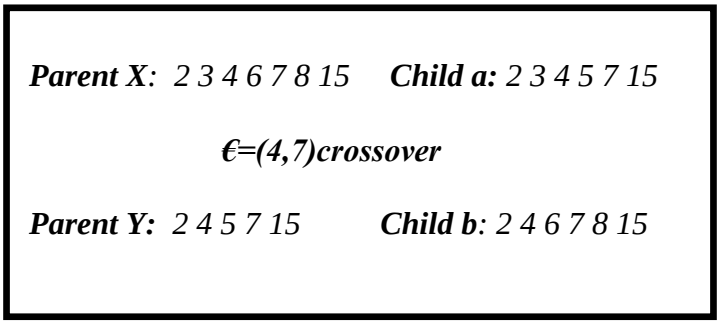


Fig.3 Modifying(Adaptive) crossover operation

The prospective research work will use either 2-bit or Modifying crossover which will figure out the path competency and eliminate the redundancy of analogous chromosomes in the originated descendants as well as redundancy of nodes in a chromosome. This perpetuates originality of a node in a chromosome. To conclude, the crossover operation bestow the competent 'r' chromosomes.

3.4 Necessity of Biometrics Security

Security requirements are quite demanding for mission-captious applications such as a military , access control and monitoring therefore secure protocol developed for ad-hoc network must combine both biometrics and cryptography techniques embedded with meta-heuristic algorithm to make the system more secure. Biometrics ,clearly is the evaluation and employment of the exclusive features of humans beings to categorize from each other. Biometrics exemplify the approaches for exclusively diagnosing human behavioural traits which fall under the categories of **strong biometrics** that acquire high distinctive content and great extent of stability, like fingerprints, DNA, iris, retina, etc , whereas **weak biometrics** possess low distinctive content and changes gradually, like hand-geometry, face, keystroke dynamics, etc. The indulgence amid the various biometric technologies brandish on the application and security . The strong biometric technologies that can readily be adaptable in MANET are fingerprints and iris recognition. From many years fingerprints and iris have been propitiously used in human identification due to their resolute and unique nature throughout human life. Biometrics are conferred as congenital identification tool that cannot be acquired, stolen, or jilted, and duplication is impractical hence provide greater security and authentication in MANET. Although biometric provide number of advantages some security and privacy apprehensions still can occur:

- ►Biometric can be genuine but not necessarily private(secret).
- ►Eliminating or abolishing biometric is not possible.
- ►If once lost, biometric are exposed permanently.
- ►To apprehend humans, cross-matching is employed barring their approval.

Consequently impinging the constraints of biometrics as discussed , some features of original biometric are taken and transposed using meta-heuristic algorithm. If anyhow arbitration of biometric takes place , retraction is done by adopting different property set and distinct genetic procedure, hence conserving continuity and confidentiality of the biometric.

4. PROBLEM IDENTIFICATION

4.1 Procreation of Intelligent Optimization-Stationed Crypt- Biometric approach by employing Iris Connotation Process(ICP)

Developing a secure protocol to sustain optimization and trust in MANET through crypt-biometric approach inculcating meta-heuristic based genetic algorithm is the main objective of our study. Our approach basically exploits features of meta-heuristic algorithm both for optimizing MANET by attaining Quality of service(QOS) and overcoming privacy concerns of biometrics.

For exploiting intelligent optimization technique for Quality of service(QOS) formulated accession problem, we led to develop an approach for concealing solutions as viable chromosomes so that the operator (crossover) leads to viable chromosomes which tends to result in attainable chromosomes [8]. The prospective technique focuses in recognizing permutation encoding mechanism for chromosome illustration. This technique causes distinct genetic code of a chromosome to proceed an identification of a node where neither node can recur over again in the corresponding chromosome.

In the prospective research work every node in MANET cultivate biometric impressions of each and every other node. The prospective secure protocol can exploit both fingerprint and iris specifications but in this research work strong biometric i.e. iris will be exploited. If a source node transfers a message to any destined node, the source undergoes an iris connotation process(ICP) which starts with procurement of eye. Images are refined to align the scale and radiation of the iris and localize the iris pattern .Then follows feature evulsions which selects the fittest 'q' chromosomes for crossover. Selected chromosomes undergo 2-bit/ modified(adaptive) crossover operation as depicted in fig.3.If required , percolate mutation operation with lowest probability which results in generating cryptographic key by employing either Fiestel or DES key generation algorithm Receiver exploits his biometric to institute the corresponding cryptographic key and the similar genetic operations are employed for decryption as well. A new key is generated by applying the above mentioned procedure if the generated biometric stationed key is implicated.

4.2 Objective of the Study

The research work is formulated as follows:

►Introduction deals with the background and originality of the approach , focusing on ad-hoc network its security challenges and various existing secure routing protocols for MANET.

►Literature survey focuses on various papers rendered towards security of MANET, cryptography and meta-heuristic algorithms.

►Broad area of research analyze the area of research that explains the concepts of Quality of service(QOS), Intelligent Optimization algorithms, and Biometric technique.

►Problem identification specifies procreation of intelligent optimization-stationed crypt-biometric approach by employing Iris Connotation Process(ICP) and objective of the study summarizes the main objectives of this research.

►Methodology to be adopted specifies the algorithm for achieving QOS and trust.

►Proposed/expected outcome of the research deals with the implementation and simulation framework.

►Last section of this short synopsis deals with various references exploited in our approach .

5.METHODOLOGY TO BE ADOPTED

5.1 Proposed Algorithm For Achieving QOS

► Firstly, percolate the initialization of the various original chromosomes which are all possible set of routes.

►Secondly, rerun the procedure un-till expired.

►Thirdly, fitness interpretation of all persuasive chromosomes following the fitness function.

► Fourthly, percolate selection operation from figured out chromosomes by applying rank selection technique.

►Fifthly, percolate crossover operation by applying 2-bit or modifying(adaptive) crossover techniques.

►Sixthly, percolate mutation operation with lowest probability.

►Seventhly, relinquish the above mentioned steps until optimization is achieved.

►Lastly, return back to step 2 up till terminated.

Originally, entire associated paths from particular source(S) to destination(D), which are referred as the engendered chromosomes are accomplished . To formulate the initial population the ‘p’ figured chromosomes are chosen irregularly from the engendered chromosomes by computing the fitness of every chromosomes in the population .One of the key technique of selection operation namely, ranking selection selects the fittest 'q' chromosomes. 2-bit or modifying crossover (any one to be exploited) analyze the fittest chromosomes and remove the redundancy of analogous chromosomes in the produced descendents .Consequently fitness interpretation and recurrence analysis are conducted in ‘F’ number of stages to acquire the finest optimized path hence achieving QOS in MANET.

5.2 Process Describing Fundamental Population Engenderment And Chromosome Embodiment

In the prospective algorithm the genetic code exemplify the node while the chromosome exemplify the network direction. The population which is the key input in this prospective approach is the assemblage of ‘m’ conceivable paths from a particular source(S) to a particular destination(D) are aggrandized irregularly from a developed Route List(RL). Hop count of a

particular path is specified as (t - 1) where t is the absolute representation of nodes in that particular path.

5.3 Fitness/Competency Interpretation of the Generated Population

Meta-heuristic algorithm investigates the most favourable route with preeminent fitness/competency. The fitness/competency function is employed to estimate the superiority of the accustomed itinerary amidst the population [5]. This function is exploited arithmetically to assess the superiority of every chromosome in the population.

The fitness/competency function is elucidated in the equation described below:

$$\blacktriangleright f_{i=} \sum_{i=1}^{hop} \mu_i(M) * \sigma_i(M) * \beta_i(M)/b * \sum_{i=1}^{hop} \mu_i(M) * \omega_i(M)$$

where

► $\mu_i(M)$ = count (A[M][j] < λ)/m:classical achieved authenticity relationship of the node 'M'.

► λ *:* the minimal recommended reliability for mutating the packets [5].

►$\sigma_i(M)$ = count (B[M][j] =1)/m : classical packet transference progress relationship of the node 'M'.

► $\beta_i(M)$ *:* the competency of node 'M'.

►*b:* the range of packet.

►$\omega_i(M)$ *:* bit interval of node 'M'.

The ranking selection method selects the fittest 'q' chromosomes for crossover.

5.4 Proposed algorithm for Crypt-Biometric Approach Inculcating Meta-heuristic algorithm

The proposed algorithm for crypt-biometric approach inculcating meta-heuristic algorithm is described below:

1.If a source node transfers a message to any destined node, the source undergoes an iris connotation process(ICP) shown in fig.4 which starts with procurement of eye.

2.ICP(Iris Connotation Process)

***Refining**

The attained image perpetually contains not only the effective component (IRIS) but may also include some components like eyelid, pupil & reflection which are not propitious for our work. Circumstances like the illumination not regularly scattered, distinct eye-to-camera purview may conclude distinct image dimensions regarding same eye. So refining undergoes a iris dissolution process which exploits Daugman's integro-differential operator for ascertaining iris as well as pupil contour [26] which is illustrated by the given equation:

$$\mathrm{Max}_{(r,x0,y0)} \left| G_\sigma(r) * \partial/\partial_r \int r,x_0,y_0\, I(x,y)/2 \right| \prod \mathrm{r\ ds}$$

Where:

► r,x_0,y_0: This is specified as the centre and radius of coarse circle (it is referred for each pupil as well as iris).

► $G_\sigma(r)$: This is the Gaussian function.

► ∂_r: This is the radius extent (range) utilised to penetrate I(x, y) of the initial iris image.

Iris localized structure is altered through Daugman's dissolution algorithm from cartesian to polar coordinates. Intensification of the image is carried out by histogram equalization method.

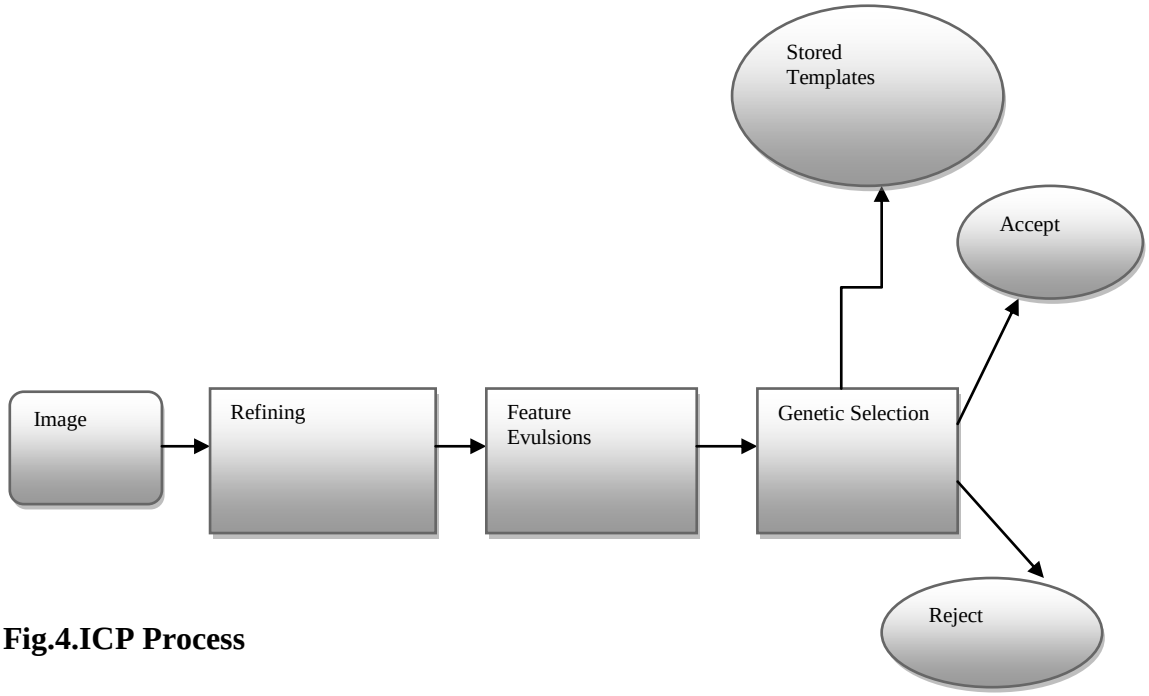
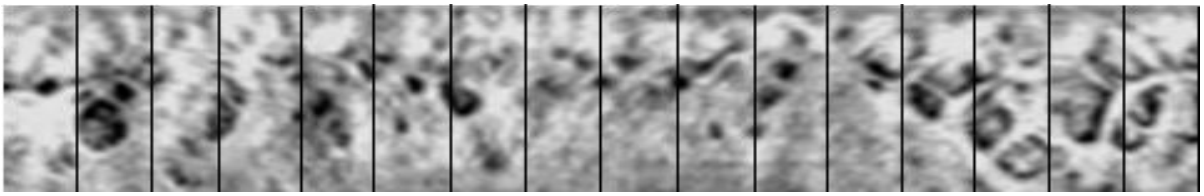


Fig.4.ICP Process

***Feature Evulsions**

Feature evulsions is the most important process which includes iris cipher propagation for converting a two dimensional image into arithmetic framework (fig.5), shows dissolution of iris image into primary cell range for propagation of iris cipher. Pixels undergo standard deviation which is exploited as an exemplary value of a primary cell region for estimation. We evolve 16 bit values which need to be transformed ,contemplating the boundary value as mean against all blocks. Make pixel value 1 if their original value is larger than boundary value otherwise a 0.

e.g. Iris Code :1 0 1 0 0 1 0 0 0 1 1 1 1 1 1 1



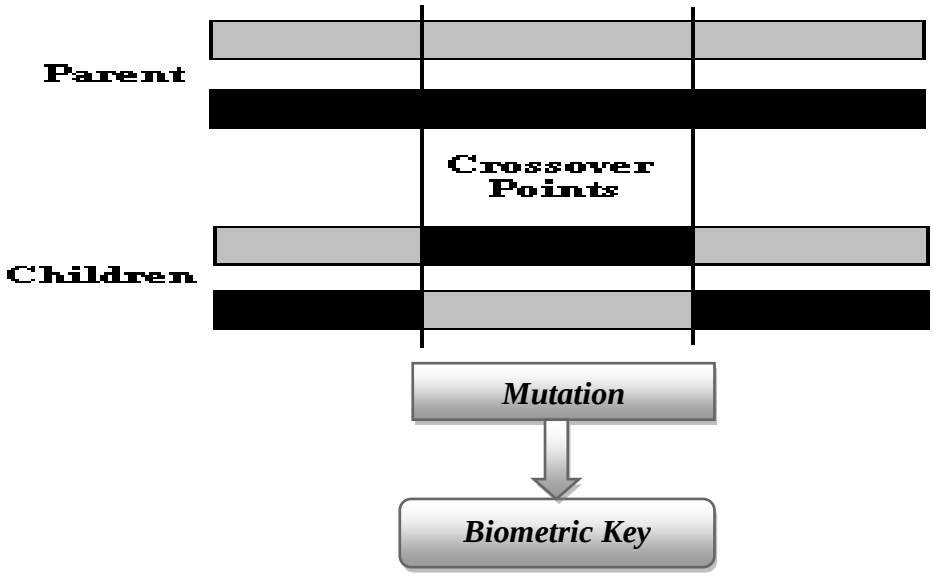


Fig.5. Generation of biometric key from refined iris image by applying meta-heuristic algorithm

Next generating the hamming length(distance) amidst two bit templates to draw a conclusion whether the two templates were from distinct or same irises.

Hamming length amidst two strings is the analogous bit positions difference between them.

```
    A       0 1 0 0 1 0 1 0 0 0
    B       1 1 0 1 0 1 0 1 0 0
A XOR B = 1 0 0 1 1 1 1 1 0 0
```

Fig.6. Hamming Code for 2 strings

In fig.6 the hamming code amidst the above 10-bit strings is 6 ie. the number of 1's in the XOR string .The iris is correlated to earlier accumulated iris code to enumerate the hamming distance amidst them. Number of bits difference between two iris code is the hamming distance between them. Hence the hamming distance of an iris code to itself is 0, to its complement is 1 and (expected distance) between 2 random iris codes is 0.5.

3.Accomplish crossover operation of by executing 2-bit or Modifying(Adaptive) crossover techniques.

4.Carry out mutation operation with lowest probability if required.

5.Thus by applying the above mentioned operations a cryptographic key is produced by employing either DES Fiestel network or AES key generation.

5.Relinquish the above mentioned steps until optimization is achieved.

5.5 Establishing Trust Forwarding Scheme

Trust is established in ad-hoc network through our prospective, approach by maintaining a trust weigh sustained for each node hence provide assistance in packet transmission. Each interposed node imprint the packets by enumerating its melange (hash)weigh and advances the packet pointing to the required destination(D)node. The required destination(D) node substantiate the melange weigh and investigates the trust weigh. If the melange(hash) weigh is substantiated, the trust weigh is enumerated, alternatively it is reduced. If the trust weigh value falls below a trust extreme, the equivalent node is imprinted as malignant. Trust standard is maintained by using Cipher Block Chaining (CBC) Mode of AES(Advance Encryption Standard) algorithm. The algorithm establishes encryption/decryption and certification of packets in a single-passage process which slashes the estimation sustenance partly, rather than determining them exclusively, thus the communication sustenance(overhead) is abridged significantly. The prospective research focuses in strenuously estimating the nodes trust weigh values. Quality of Service which is the key requirement of our algorithm is maintained when the particular source(S) node is able to choose the more trusted route rather than choosing the

shorter routes. The potential damage is avoided in the prospective protocol by marking and segregating the malignant nodes and prohibiting them from competing in the network.

A Trust Counter List(TCL) is perpetuated by all nodes in the network node. Certify {Tcl1,Tcl2 ,.....} as the fundamental trust count of the nodes{n1, n2 ,.....} preceding the route R from a particular source (S) to a particular destination (D). Nodes can neither be thoroughly trusted nor be dis-trusted as they do not have any information about the reliability of their neighbours in the beginning, Route Request Packet(RREQP) is send when a source node (S) wants to institute a route to the destination node (D).All nodes in a network keep a record of the aggregate of packets it has delivered over a route employing a deliver counter (DC).

Every time, when a node *ni* apprehends a packet from a node *nj* ,then *ni* aggravate the deliver counter of the node *nj*

$DC_{nj} = DC_{nj} + 1$, $j = 1,2.....$

TCL of node *ni* is transformed correspondingly according to the values of *nj* DC. Simultaneously every node impel its TCL and hence the data packets approach towards their destination(D) node. When the required destination(D) node apprehend the hoarded RREQP, it checks out the number of data packets received *Rec* hence it constructs a function on *Rec* with the key unified by the sender(S) node and the destination(D) node.The RREPP encompass the specified source(S) node and destination(D) node ids, the function of *Rec* , the hoarded route from the RREQ digitally signed by the destination. The RREPP is forwarded towards the source on the reverse route R.

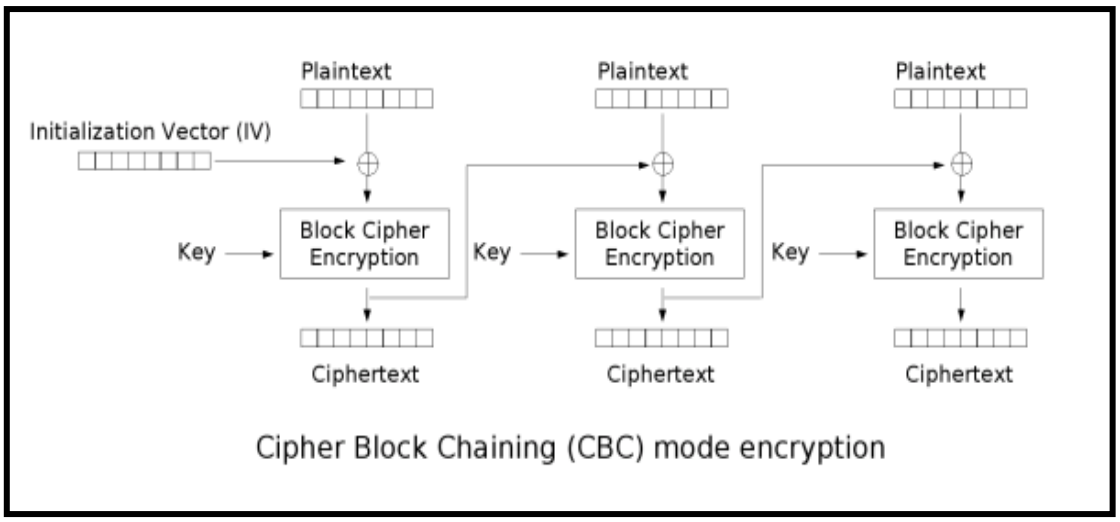


Fig.7.CBC Mechanism: Encryption Operation

Fig.7.and fig.8 embellish the elemental steps of CBC mode encryption and decryption operations.
Equation 1 represents CBC mode encryption :-

$Ci=EK\ (Pi \oplus Ci\text{-}1)\ C_0=IV$ ----------*1*
while equation 2 represents CBC mode decryption :-
$Pi=DK\ (Ci \oplus Ci\text{-}1)\ C_0=IV$----------*2*

The operation of CBC mechanism is illustrated below:

Encryption: A section (block) of cipher-text will be recurred for each section of plain-text block, for encrypting a plaintext. One or two sections will be recurred for encryption of the uttermost section of the plaintext.

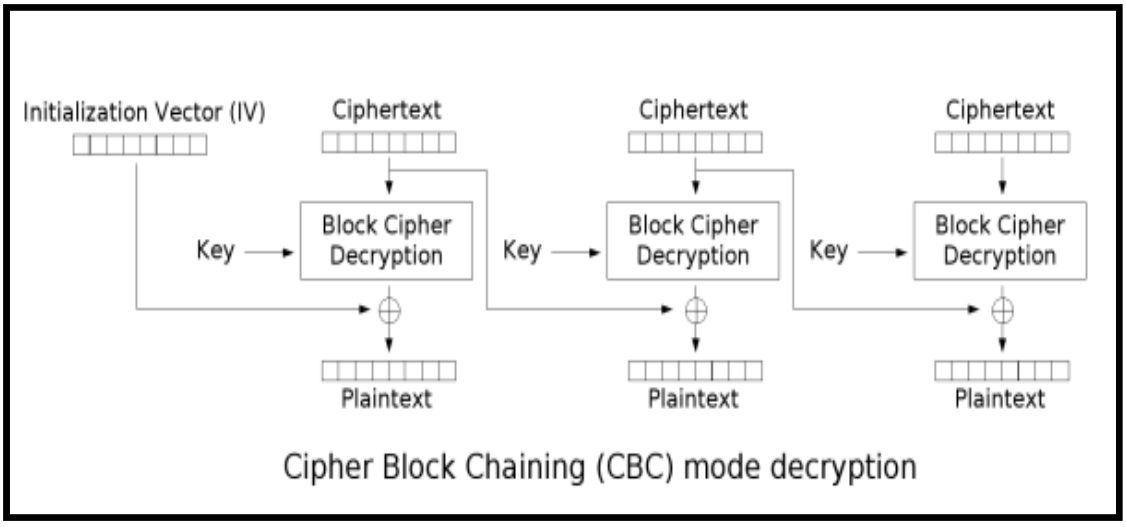


Fig.8.CBC Mechanism: Decryption Operation*:*

Decryption: Moreover, decryption proceeds just in the contra manner of encryption. Excluded, from the decryption of the uttermost block, one section of plain-text will be recurred for each section of cipher text. Succeeding the decryption of the uttermost section of plain-text , its padding bits are computed and cut-off, retracing a compelling plaintext.

5.6 Ensuring Security of Data in MANET

Ensuring security of data through our prospective secure protocol is done by applying the above developed key to encrypt the original message using a simple cryptographic algorithm . DES fiestel network or AES algorithm can be exploited. Here we will be discussing about AES method where encryption as well as decryption operations are stated by the formulae:

Cipher-text = Encryption Algorithm BGK (Plaintext)

Plaintext = Decryption Algorithm BGK (Cipher-text)

where:

BGK **-** Biometric Genetic Key (created by Recipient Biometric)

Advanced Encryption Standard(AES) is a type of non-Feistel cipher in which 10, 12, or 14 rounds are employed to encrypt as well as decrypt a data block of 128 bits in size. Key size which is contingent upon on the number of rounds can be 128, 192, or 256 bits. Various terminologies that are specified in AES are :

►**in** matrix: It is single 128 bit block(input of algorithm) utilised both for decryption as well as encryption .

►**state** array: It is a reproduction of in matrix which is altered at each level and hence reproduced as an output matrix as shown in fig.9.

►**w** matrix : It is the elaboration of the key is into an array of key schedule words .

►**Add round key:** This level records the starting of the algorithm subsequently by 9 rounds of four stages and a tenth round of three stages ,applying both for encryption as well as decryption.

The four levels of the algorithm are specified as substitute byte ,shift rows, mix columns and add round key. The tenth round directly leaves out the mix columns level. The starting nine rounds of the decryption algorithm consist of inverse shift rows, inverse substitute bytes, inverse add round key and inverse mix columns. Repeatedly, the tenth round directly leaves out the inverse mix columns level.

5.7 Security features accomplished by our proposed protocol

► **Confidentiality**: The approach targets in maintaining the privacy of the data .Consider the situation where the attacker tries to acquire the primitive directive(message) against the text which is encrypted, leads to the requirement of cryptographic key. The developed key can be acquired only through recipient biometric. Additionally the biometric is not used in its original form rather a cancellable interpretation is exploited that makes computationally inconceivable to acquire the key.

►**Authentication:** Through this proposed work, the participants of MANET corroborate every participant through their respective biometric. At the time of receiver verification of the

message to check whether or not it is through a valid sender, the message is encrypted by acquiring the sender's biometric and the receiver explores the same biometric to decrypt the message.

►**Integrity:** Integrity is maintained in through the recipient verification to check whether the received message is the actual message transmitted by the sender. If the intruder by any chance tries to change the cipher-text, the authentic plaintext will not be developed after trying to decrypt through the key created by employing recipient biometric.

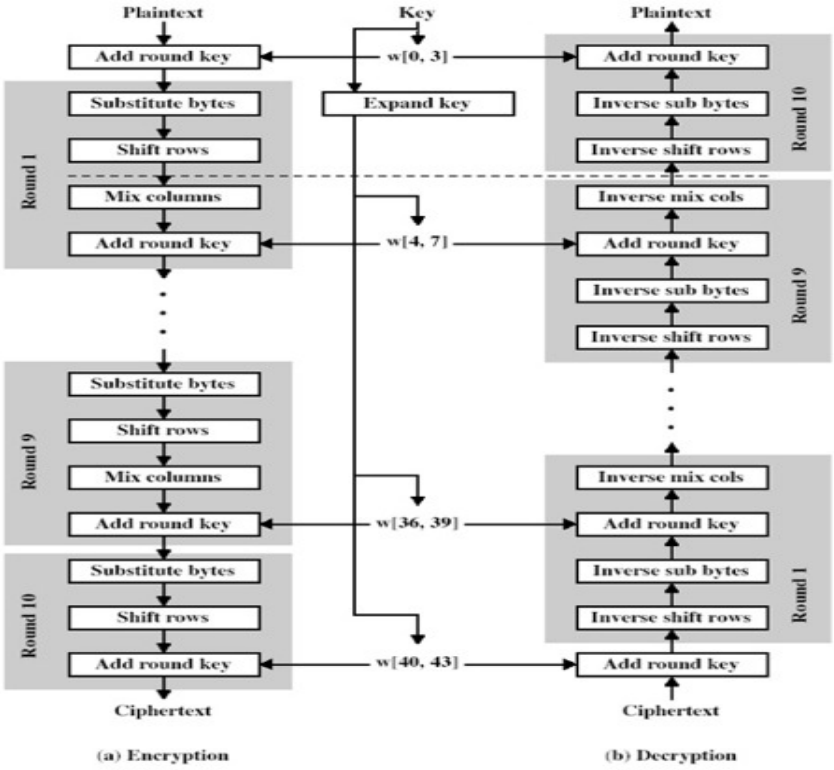


Fig 9. AES Algorithm

5.8 Expected time frame required for developing optimized secure protocol for MANET through biometric approach

The methodology discussed in above sections(5.1-5.7) for developing a secure protocol for MANET requires an expected time frame of around 12 months i.e. 4 months for each module. The modules are listed below:

►First module which deals in achieving QOS for MANET optimization using meta-heuristic algorithm.

►Developing biometric specifications.

►Proceeding towards enhancing privacy of biometrics through meta-heuristic technique.

►Lastly sustaining trust through cryptography.

6.PROPOSED/EXPECTED OUTCOME OF THE RESEARCH

The proposed research work of developing a secure protocol for MANET to sustain optimization and trust in MANET through crypt-biometric approach inculcating meta heuristic algorithm will be implemented through MATLAB platform and analyses of the simulations through NS2 .The proposed protocol will be compared with the previous secure protocols like SEAD ,SAR ,SRP etc and performances will be evaluated through various features like reduced overhead, end-to-end delay, reduced throughput enhanced levels of security, key size and time consumed in key generation, encryption and decryption of data etc .First phase of the protocol selects shortest fittest route for optimization in MANET through meta-heuristic algorithm. Every node in MANET cultivate biometric impressions of each and every other node. After discovering a fittest route if a source node transfers a message to any destined node, the source undergoes an iris connotation process and hence generates fittest offspring which then undergo various meta-heuristic operations to overcome the shortcomings of biometrics. A crypt-biometric key is produced to enhance security of MANET . Acquaintance (Confidentiality) and Corroboration (Authentication) of packets for routing in MANET is attained in the next phase of the protocol by targeting on trust application .We will be intriguing a trust based packet delivering scheme for detecting and isolating the malignant nodes using the routing layer information. A trust weigh is maintained and a node is defrocked or remunerated by decreasing or increasing the trust weigh value. If the trust weigh value falls below a trust threshold, the equivalent node is marked as malignant. Hence data is protected by applying various levels of security by our prospective approach which develops trust between various nodes of ad-hoc network. Future enhancement of the protocol will be dependent on the simulation results being analysed.

7.REFERENCES

[1] Abhishek Roy, Sajal K. Das, "QM2RP: A QoS-Based Mobile Multicast Routing Protocol Using Multi-Objective Genetic Algorithm", Center for Research in Wireless Mobility and Networking (CReWMaN),2004.

[2]Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis "Secure Routing and Intrusion Detection in Ad Hoc Networks" Third IEEE International Conference on Pervasive Computing and Communications, March 2005.

[3] Ananda Krishna.B, Radha.S and K Chenna Kesava Reddy, "Data Security in Ad hoc Networks using Randomization of Cryptographic Algorithms", Journal of Applied Sciences, pp. 4007-4012, 2007.

[4]Awerbuch.B et al., "Ad hoc On-Demand Distance Vector Routing Protocol Resilient to Byzantine Failures", ACM Wise, 2002.

[5] D.E. Goldberg, "Genetic Algorithms in Search, Optimization and Machine Learning" Addison Wesley, New York, 1989.

[6] Farooq Anjum, Dhanant Subhadrabandhu and Saswati Sarkar "Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols" in proceedings of IEEE 58th conference on Vehicular Technology, 2003.

[7]Fessi B A, Ben Abdallah, S, Hamdi Mand Boudriga, "A new genetic algorithm approach for intrusion response system in computer networks", IEEE Symposium on Computers and Communications, pp. 342-347, 2009.

[8] Guerin.R.A and A. Orda, QoS routing in networks with inaccurate information: Theory and algorithms,IEEE/ACM Transactions on Networking 7(3) (1999) 350–364.

[9]Haas.Z, J. Deng, B. Liang, P. Papadimitratos and S.Sajama Wireless ad hoc networks. In J. Proakis, editor, Wiley Encyclopedia of Telecommunications.John Wiley and Sons, 2002.

[10] Hahill.B et l., "A Secure Protocol for Ad Hoc Networks", OEEE CNP, 2002.

[11]Hao.Y et al., "Security In Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, 2004.

[12] Hu.Y, A. Perrig, and D. Johnson, "Ariadne: A secure On demand Routing Protocol for Ad hoc Networks", ACM MOBICOM, 2002.

[13] Jayraj Singh, Arunesh Singh, Raj Shree "An Assessment of Frequently Adopted Security Patterns in Mobile Ad hoc Networks: Requirements and Security Management Perspective, Journal of Computer Science and Data Mining ,Vol. 1,No. 1-2,December 2011

[14] Jie Liu, F. Richard Yu, Chung-Horng Lung and Helen Tang, "Optimal Biometric-Based Continuous Authentication in Mobile Ad hoc Networks", Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, pp. 76-81, 2007.

[15]Kil-Woong Jang"A tabu search algorithm for routing optimization in mobile ad-hoc networks, Springerlink.com,2011.

[16]Kompella.V.P, J.C. Pasquale and G.C. Polyzos, Multicast routing for multimedia communications, ACM/IEEE Transactions on Networking 1(3) (1993) 286–292.

[17]Liu, Kejun Deng, Jing Varshney, Pramod K.Balakrishnan and Kashyap "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transactions on Mobile Computing, May2007.

[18]Panagiotis Papadimitratos, and Zygmunt J. Haas,"Secure Data Communication in Mobile Ad Hoc Networks", IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, February 2006.

[19] Panagiotis Papadimitratos, and Zygmunt J. Haas, "Secure Routing for Mobile Ad hoc Networks", In Proceedings of SCS Communications Networks and Distributes Systems Modeling and Simulation Conference, CNDS 2002.

[20] Qinghan Xiao, "A Biometric Authentication Approach for High Security Ad hoc Networks", Proceedings of IEEE Workshop on Information Assistance, pp. 250-256, June 2004.

[21]Rajaram.A,S.Palaniswami"A Trust Based Cross Layer Security Protocol for Mobile Ad hoc Networks", (IJCSIS) International Journal of Computer Science and Information Security, pp.Vol. 6, No. 1,2007.

[22]Rakesh Kumar and Mahesh Kumar, "A novel routing technique for computer networks using personalized GA, (Under review process in Journal).

[23]Ramanathan.R and J. Redi. A brief overview of ad-hoc networks: challenges and directions. IEEE Communications Magazine, 40(5):20–22, 2002.

[24] Shanthini.B and S. Swamynathan "A Cancelable Biometric-Based Security System for Mobile Ad Hoc Networks", International Conference on Computer Technology (ICONCT 09), pp. 179-184, December, 2009.

[25] Tao Wan, Evangelos Kranakis, P.C. van Oorschot, "Securing the Destination Sequenced Distance Vector Routing Protocol (S-DSDV)",

[26] Wolff E. (1976) Anatomy of the Eye and Orbit.7th edition. H. K. Lewis & Co. LTD. 7th edition. H. K. Lewis & Co. LTD.

[27] Yanchao Zhang, Wenjing Lou, Wei Liu, and Yuguang Fang, "A secure incentive protocol for mobile ad hoc networks", Wireless Networks, (WINET), vol 13, No.5, October 2007.

[28] Zakir.A.H "Genetic Algorithm for the Travelling Salesman Problem using Sequential Constructive Crossover Operator" International Journal of Biometrics & Bioinformatics (IJBB), 2004.

[29] Zarza L., Pegueroles J and Soriano M "Interpretation of Binary Strings as Security Protocols for their Evolution by means of Genetic Algorithms.